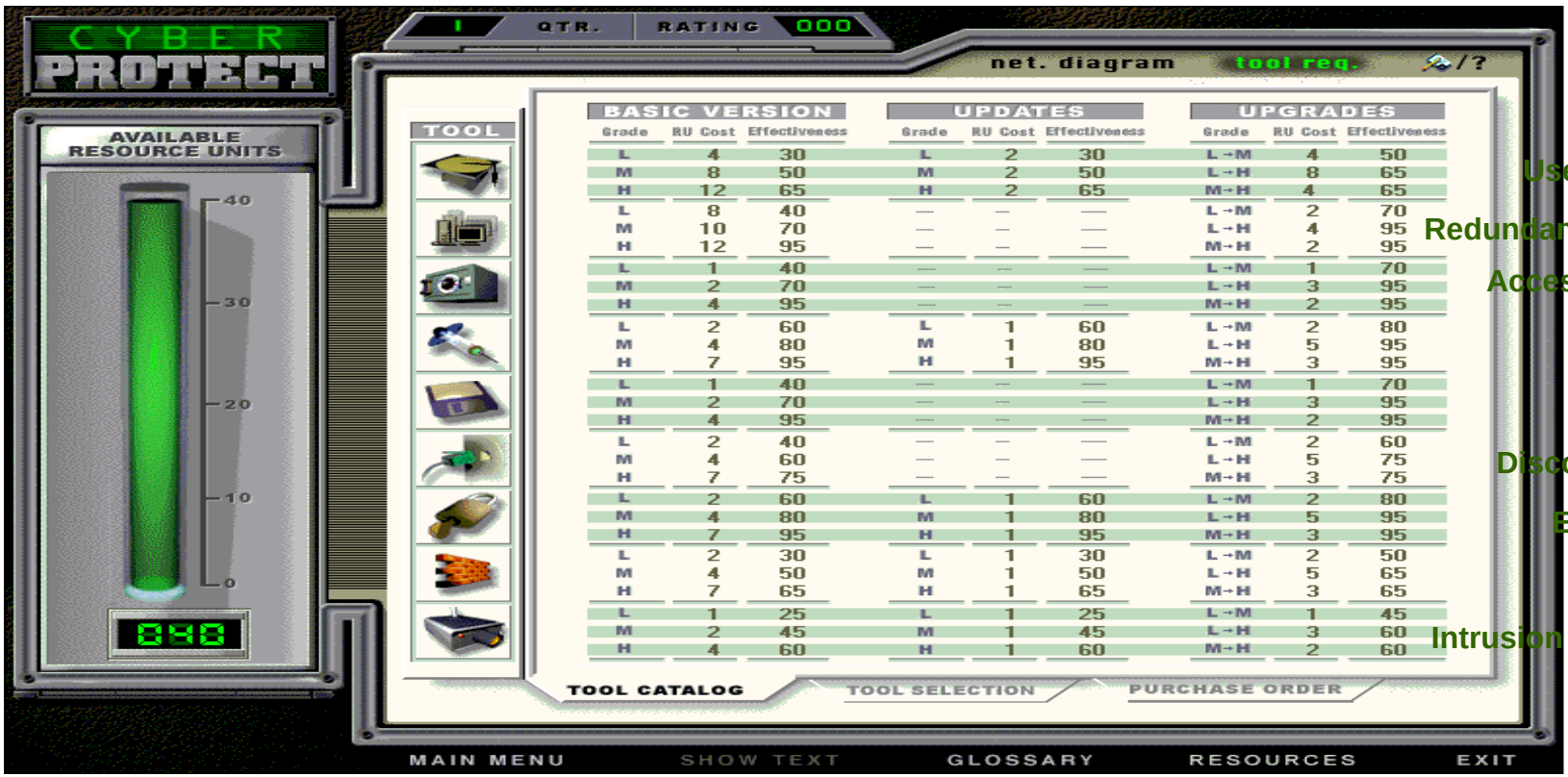
Teine küsimus oli –
kuidas jagada saadud mõttekas kulutus infoturbe tegevusvaldkondade vahel ?

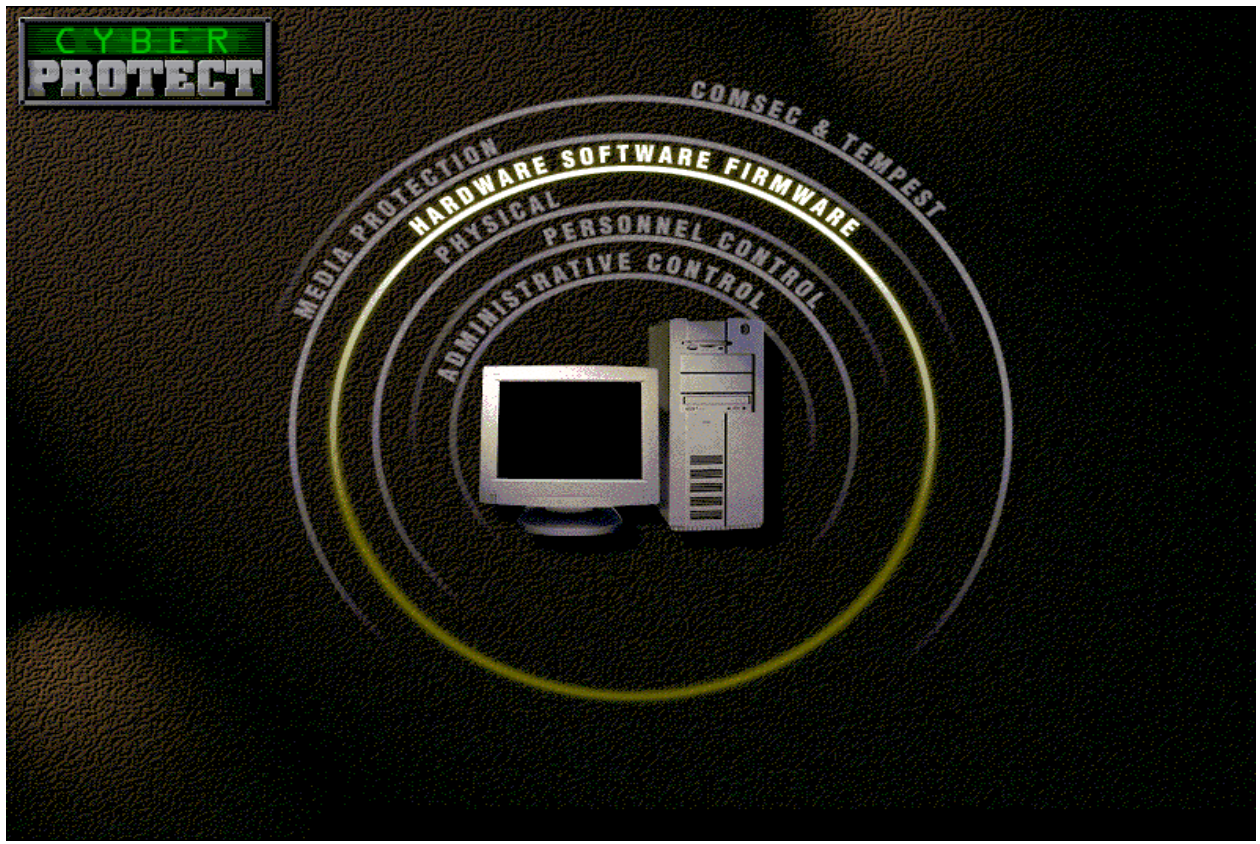
1. Cyber Protect

Defense Information Systems Agency,
US DoD, US Military Academy

Eeskujuks sobiks USA Sõjaväeakadeemia infoturbe õppevahend/interaktiivne mäng CyberProtect – ainus materjal, kus mina olen kohanud teatud infoturbemeetmete reaalseid efektiivsusnäitajaid.



Muidugi on sõjaväelaste metoodika tunduvalt täielikum, kuid mängus on aluseks võetud eeldus, et teistes turvavaldkondades on kõik juba suurepäraselt tehtud.



Mänguga mingeid arvutusmetoodikaid kaasas pole, kuid (lihtsustatult) võiks oletada midagi järgnevat:

Mitteefektiivsus = ÕnnestunudRünded / KõikRünded x 100%

Efektiivsus = TõrjutudRünded / KõikRünded x 100% =
(KõikRünded – ÕnnestunudRünded) / KõikRünded x 100%

Kogu süsteemi efektiivsus = allsüsteemide efektiivsuste aritmeetiline keskmine (max ~82%) (kehtib juhul kui kõiki süsteeme võrdselt rünnatakse).

Rumal oleks mingis valdkonnas kulutusi üldse mitte teha – selle valdkonna efektiivsus oleks “0” ja kogu süsteemi efektiivsus langeks märgatavalt.

Infoturbe kulutuste otstarbekuse määratlemiseks võiks kasutada midagi sellist:

Cost-Effectiveness = Cost / (X-Y) , kus
Cost-Effectiveness – ühe ründe ärahoidmiseks kulunud raha,
Cost – turbeks kulutatud raha,
X – õnnestunud ründed ilma kaitseta (st ilma raha Cost kulutamata),
Y – õnnestunud ründed kui kaitseks kulutatud Cost raha.
Benefit:Cost = V / Cost-Effectiveness , kus
V – keskmine kahju õnnestunud ründest kui kaitseks kulutusi pole tehtud

St kulutused mõttekad kui Benefit / Cost > 1.

Kogu probleem taandub optimeerimisülesandeks, kus mõttekad kulutused aastas on teada ning tuleb määratleda alamtegevuste tasemed selliselt, et kogu infoturbe tõenäosus tuleks maksimaalne.

Excel'is Visual Basic'u makro tegi selle töö ära:

									82,22222	= Max turvatase
12	12	4	7	4	7	7	7	4	64	= Max kulud
H	H	H	H	H	H	H	H	H		
Taining	*Redundance*	*Access Control*	*Antivirus*	*Backup*	*Disconnection*	*Encryption*	*Firewall*	*Intrusion Detection*		
0	H	H	M	H	M	M	M	H		
0	12	4	4	4	4	4	4	4	40	= Reaalne raha
									68,33333	= Optimaalne turvatase

Tulemus iseenesest vägagi huvitav ja mitte eriti andmeturbe põhialustega kokkulangev – koolitusega pole üldse mõtet tegeleda (?).

Teemast veidi kõrvale, aga huvitav - peagi sattusin artiklile, mille autor just kasutajate koolitust rumalaks ettevõtmiseks peab:

Kuus rumalaimat ideed arvutiturvalisusest

Turvalisusega võib kergelt alt minna, kui jälgida mõnd ideed, mis eirab arvutiturvalisuse põhimõtteid, kuid on sellest hoolimata kasutajate seas ülipopulaarne. Tulemüüride looja Marcus Ranum saab pidevalt kutseid erinevatele turvalisust käsitlevatele seminaridele, see teema on endiselt kuum. Kuid miks?

Üks põhjustest, arvab Ranum, ongi needsamad rumalad, reaalsust eiravad otsused ja ideed, mis olulisuse (või rumaluse) järgi ritta pannes oleks järgmised:

- vaikimisi ligipääs
- loendatud „pahad tegevused”
- „sissemurdmine-parandamine” tsükkel
- "häkkimine on lahe" suhtumine
- **kasutajate harimine**
- tegevus on parem kui tegevusetus.

Lähemalt saab lugeda kuuest rumalaimast ideest arvutiturvalisuse alal Marcus Ranumi artiklist (http://www.ranum.com/security/computer_security/editorials/dumb/).

Planeerimisülesannete lahendamiseks (ja operatsioonianalüüsi ülesannete lahendamiseks üldse) on olemas nii hinnalt kui võimekuselt mitmesugust tarkvara, kuid ühte neist tuleks eriti esile tõsta, kuna see on üldkättesaadav ja kasutatav koos MS Exceliga. Tegemist on firma Frontline Systems, Inc. poolt arendatud ja juba kümmekond aastat tagasi Exceliga liidetud programmiga Solver, mis võimaldab lahendada nii lineaarseid (LP) kui ka mittelineaarseid planeerimisülesandeid.

Solver on täiendprogramm, mis tuleb tavaliselt Excelisse eraldi paigaldada, valides ta Tööriistad -> Lisamoodulid alt (Tools -> Add-Ins) või ka vajadusel Office'i algkettalt.

SOLVER.XLA - C:\Program Files\Microsoft Office\Office10\Library\Solver

Käivitage Solver : Tööriistad -> Solver (Tools -> Solver)

Since its introduction in February 1991, the **Microsoft Excel Solver** has become the most widely distributed and almost surely the most widely used generalpurpose optimization modeling system.

Kuid meie mittepidevat ja mittelineaarset optimeerimisülesannet see Solver lahendada ei oska.

Solver'i laiendatud ja eraldi müüdav versioon (www.solver.com) **sai aga hakkama:**

The **Premium Solver Platform**, our most popular product, greatly extends the power of the Solver in Excel, which we developed for Microsoft.
It solves problems up to 10 times larger, and many times faster than the standard Excel Solver, and it handles new kinds of problems with its built-in Evolutionary Solver and new 'alldifferent' constraint type.

With plug-in Solver Engines for the Premium Solver Platform, you can solve extremely large linear programming, mixed-integer programming, smooth nonlinear optimization, global optimization, and even non-smooth optimization problems.

Our Solver DLL Platform products provide similar capabilities for your custom application program written in Visual Basic, C/C++, or any other Windows programming language. And we make it easy for you to distribute our Solvers with your application.

2. Analüütiline HierarhiaProtsess

AHP, Thomas Saaty

Põhimõtteliseks lähenemiseks on CyberProtect vägagi heaks ideede allikaks, kuid ameeriklaste kümme aastat vanad numbrid pole kindlasti need, mida aluseks võtta.

Samas võib Interneti põhjatutest infosügavustest, piisava aja ja püsivuse korral, ka midagi tunduvalt ajakohasemat välja kaevata.

Kui see aga ei õnnestu, siis tuleb intuitsioon appi võtta ja ka selleks on olemas sobiv metoodika ning seda toetav tarkvara – äripoole intuitiivsetele ekspertarvamustele analüütika lisamiseks kasutatakse analüütilist hierarhiaprotsessi (AHP, väljatöötajaks Thomas Saaty) ja "Expert Choice" programmipaketti, mida nii T. Saaty kui ta põhipartner E. Forman kasutavad ja mida võib ka üheks kuuks proovikasutuseks tasuta võrgust laenata, kartmata BSA kallaletungi.

Eestis: Leo Võhandu on kirjeldanud metoodikat A&A 04/2000's ja EBS'is tegi Märt Tars 2004.a. bakalauruse töö "ÄRIPROTSESSIDE RISKIHINNANGUD ANDMETURBE KORRALDAMISEL INFOVARADE VÄÄRTUSE MÄÄRATLEMISEKS".

Saaty soovitab kahe variandi võrdlemisel lihtsat skaalat:

- **võrdtähtis - 1**
- **mõõdukas paremus - 3**
- **oluline paremus - 5**
- **väga tugev paremus - 7**
- **ekstreemne paremus - 9**

Kui variandid A ja B on võrdselt vastuvõetavad, siis saavad mõlemad kaaluks 1.
Kui A on B-st mõõdukalt parem, siis A = 3 ja B = 1/3 (tegu on pöördvõrdelise suhtega a R b**).**
Mõõt 7 tähistab praktikas tõestatud paremust ja
mõõt 9 on lausa absoluutne tõde (umbes selline, et "päike tõuseb idast").

Olgu antud n varianti V_1, V_2, … , V_n, mida meil tuleb järjestada olulisuse või tähtsuse järjekorras. Kui me variantidel pole objektiivselt määratud omadust nagu hind või mõni muu mõõt, siis lepime eespool toodud Saaty skaalaga.
Varasemale lisaks märgime, et paarisarvud 2, 4, 6, 8 on varutud selle juhtumi jaoks, kui me ei oska eelistuse astet sisetunde põhjal täpselt määrata ja peame andma vahepealse hinnangu.

Toome näitetabelina lihtsa 3 x 3 tabeli:

	V1	V2	V3
V1	1	3	6
V2	1/3	1	2
V3	1/6	1/2	1

See tabel ütleb, et V_1 on mõõdukalt parem V_2-st ja peaaegu tugevalt parem V_3-st. Variant V_2 on omakorda veidi parem V_3-st.

Selliste suhete vahekorraga väärtuste tabel on üpris tavaline. Praegusel juhul on meil aga tegemist nn ideaaltabeliga, mis võimaldab üsna täpselt ja üsna lihtsalt võrrelda variante omavahel. Vaatame ja veendume, et risttabeli teise rea elemendid saame esimesest reast selle rea iga elementi lihtsalt kolmega jagades ning kolmanda rea saame esimest rida kuuega jagades.

Teisisõnu $V1 = V1$

$V2 = 1/3\ V1$

$V3 = 1/6\ V1$

Liites nüüd kõigi kolme rea hinnangud, saame

$V1 + V2 + V3 = (1 + 1/3 + 1/6)V1.$

Et edasises oleks kergem töötada ja keerulisemate valikuprobleemide puhul kergem võrdlusi teha, võtame kõigi variantide väärtuste kogusuuruseks ühe – st $V1 + V2 + V3 = 1.$

Seega $1 = (1 + 1/3 + 1/6)V1$ **ja siit**

$V1 = 6/9$

$V2 = 2/9$

$V3 = 1/9$

Pärast väikest rehkendust saame kõigi kolme variandi suhtelised kaalud:

$V1 = 0{,}667$; $V2 = 0{,}222$; $V3 = 0{,}111$

Teine asi, mida me selle ideaaltabeli puhul näeme, on hinnangute loogilisuse kontrolli võimaldav asjaolu, et $a_{ij}a_{jk} = a_{ik}$ **kõikide i, j, k kolmikute puhul. Näiteks** $a_{31} = a_{32} \times a_{21} = 1/2 \times 1/3 = 1/6.$

Kuid tundub, et läheb vägagi raskeks kui hakata kogu infoturvet AHP-ga kirjeldama.

Ja jälle – kus häda kõige suurem, seal abi kõige lähemal!
Abi tuli naaberlaua tagant – Enn Tõugu ja Andres Ojamaa pakkusid välja CoCoViLa ning otsustasime teha ise "Astmelise andmeturbe ekspertsüsteemi (Graded Security Expert System)" - nn tehisintellektil põhineva andmeturbe optimaalsete kulutuste määratlemise lahenduse.

Tehisintellekt kõlab veidi liiga ambitsioonikalt ja seda pole arvutitele veel suudetud (ilmselt õnneks) anda.

CoCoViLa on raamistik visuaalsete programmeerimiskeskkondade loomiseks. CoCoViLa projekt sai alguse Ando Saabase magistritööst milles pakuti välja metoodika visuaalsete spetsifitseerimiskeelte realiseerimiseks ning mille praktilises osas loodi koostöös Pavel Grigorenkoga vastavat arhitektuuri toetava arendusvahendi prototüüp.
CoCoViLa - http://www.cs.ioc.ee/~cocovila/

3. Graded Security Expert System

CoCoViLa, tehisintellekt (?).

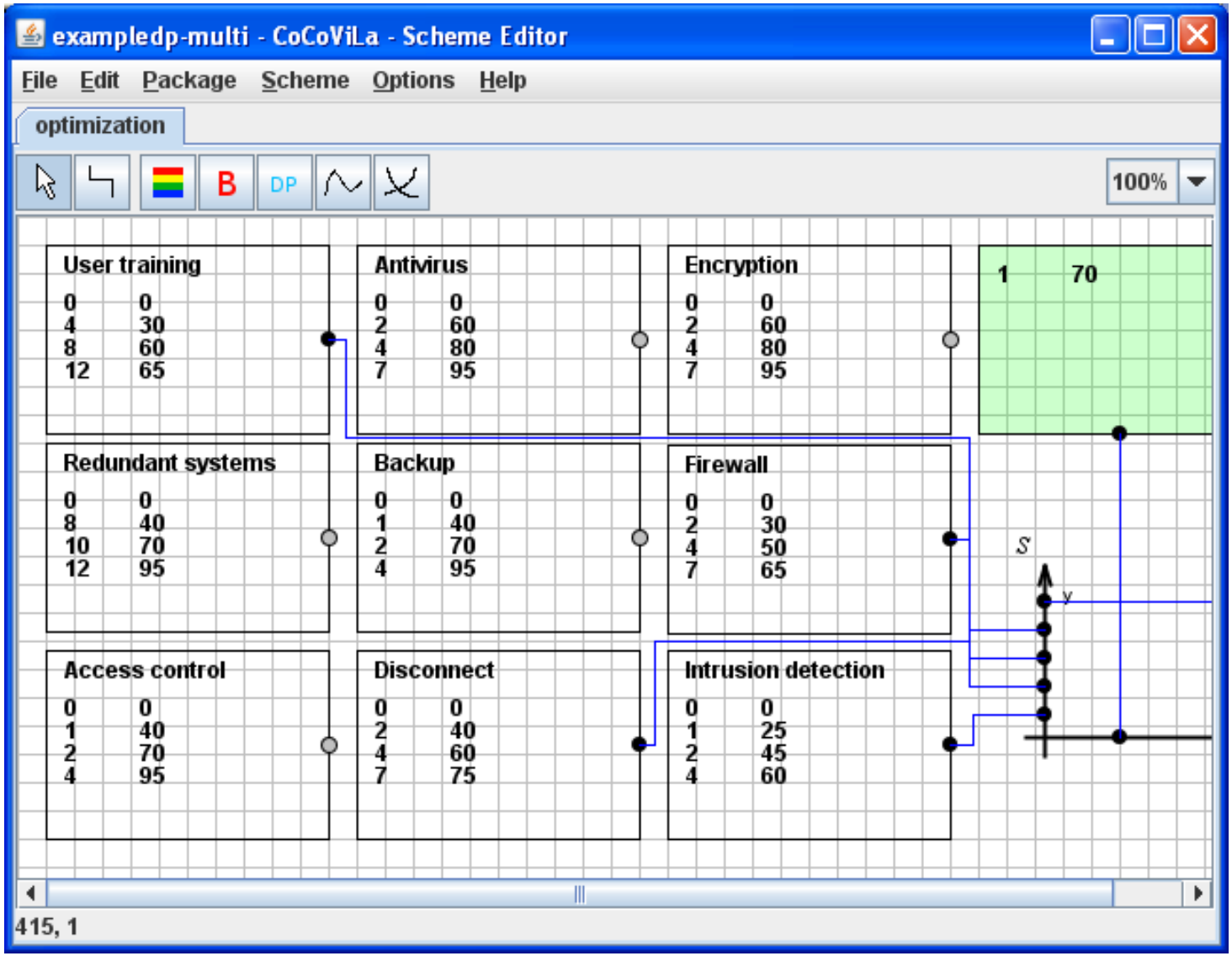
CoCoViLa provides a framework for developing visual specification languages. It includes a visual editor for drawing the schemes and a synthesizer for generating a Java program from the scheme and the class specifications.

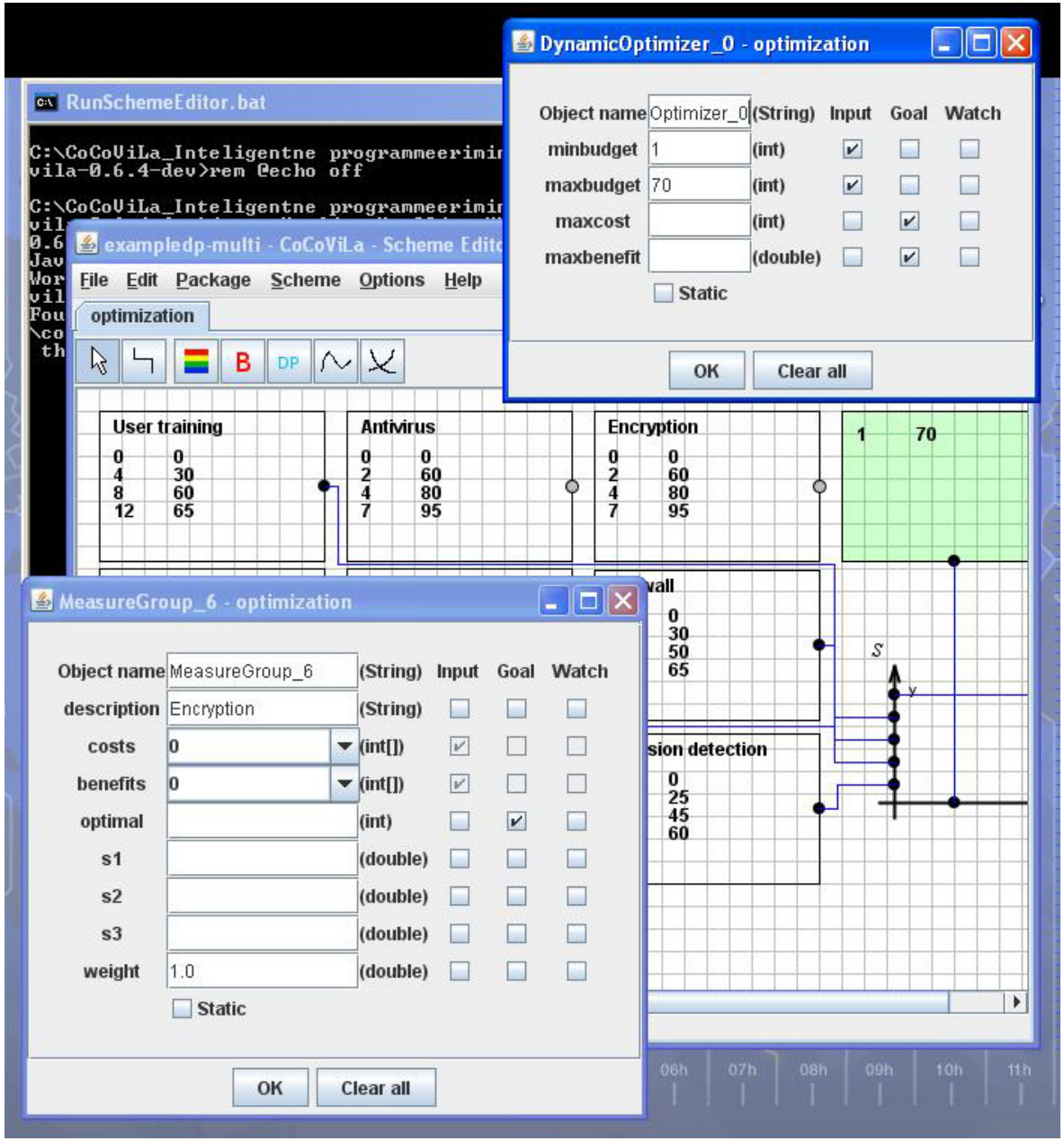
Running the program

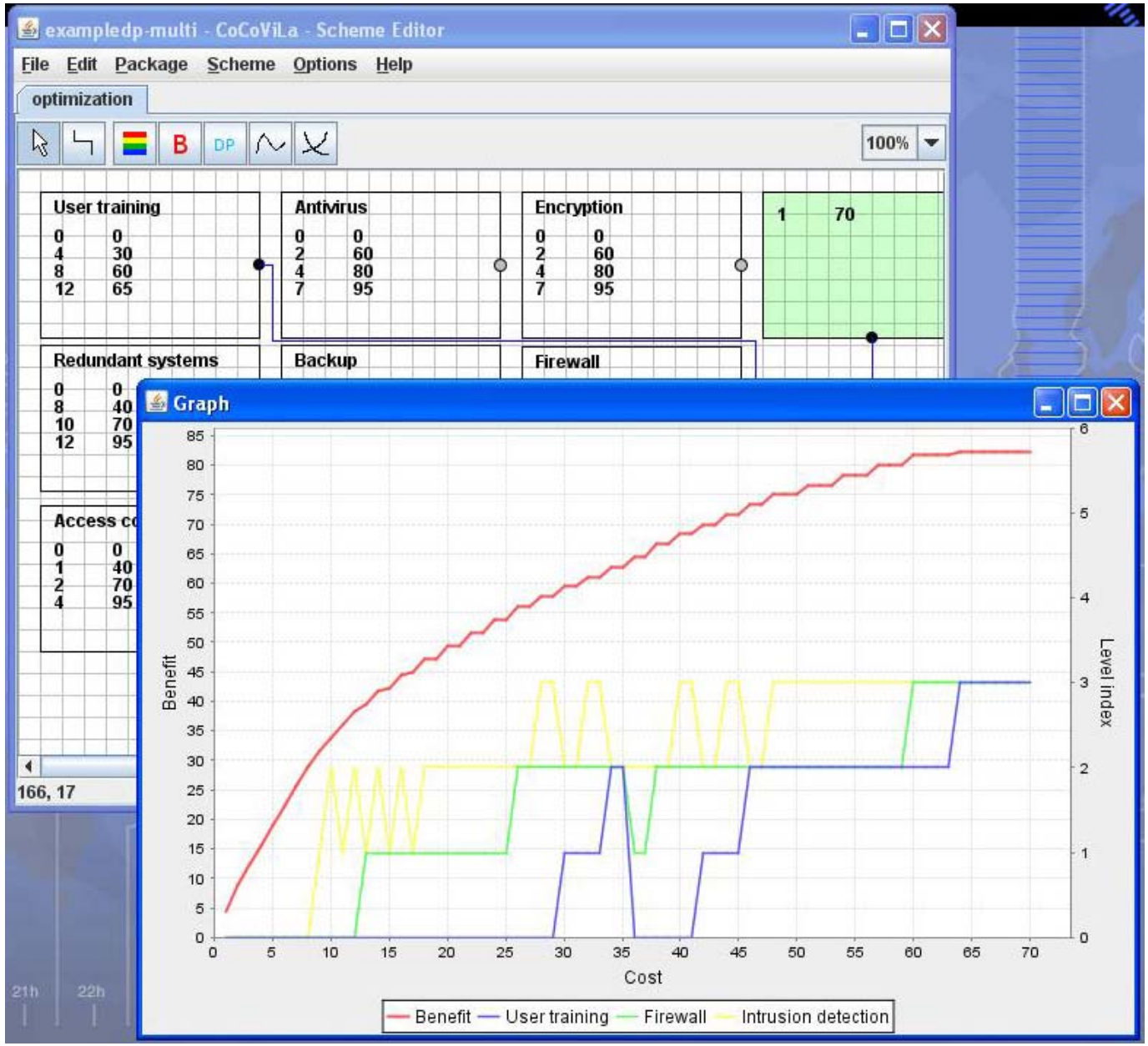
•CoCoViLa requires at least Java Runtime Environment 1.5 to run. It requires Java SDK to use the generated programs at runtime (they need to be compiled with javac). Note that for this, javac should be in the path. Installation instructions for Java can be found in http://java.sun.com/j2se/1.5.0/install.html . To run the program, execute SchemeEditor.bat. To draw the class images, use ClassEditor.bat.

Getting started

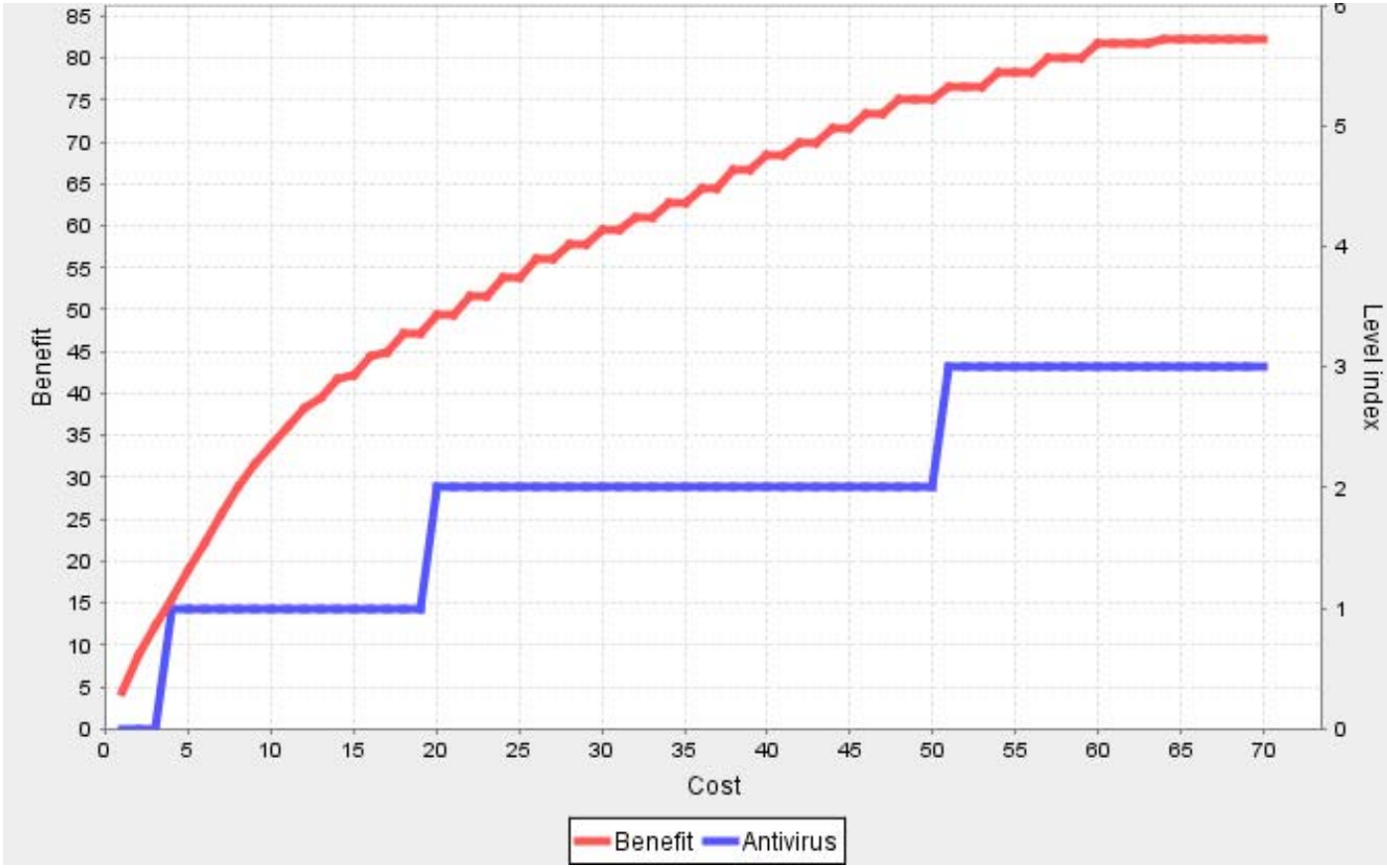
•A simple tutorial of using the editor can be found in the tutorial. The 'packages' directory includes some sample packages (files with "xml" extension), together with some schemes ("syn" extensions).


exampledp-multi - CoCoViLa - Scheme Editor
File Edit Package Scheme Options Help
optimization
B
DP
100%
User training
0 0
4 30
8 60
12 65
Antivirus
0 0
2 60
4 80
7 95
Encryption
0 0
2 60
4 80
7 95
1 70
Redundant systems
0 0
8 40
10 70
12 95
Backup
0 0
1 40
2 70
4 95
Firewall
0 0
2 30
4 50
7 65
S
y
Access control
0 0
1 40
2 70
4 95
Disconnect
0 0
2 40
4 60
7 75
Intrusion detection
0 0
1 25
2 45
4 60
415, 1

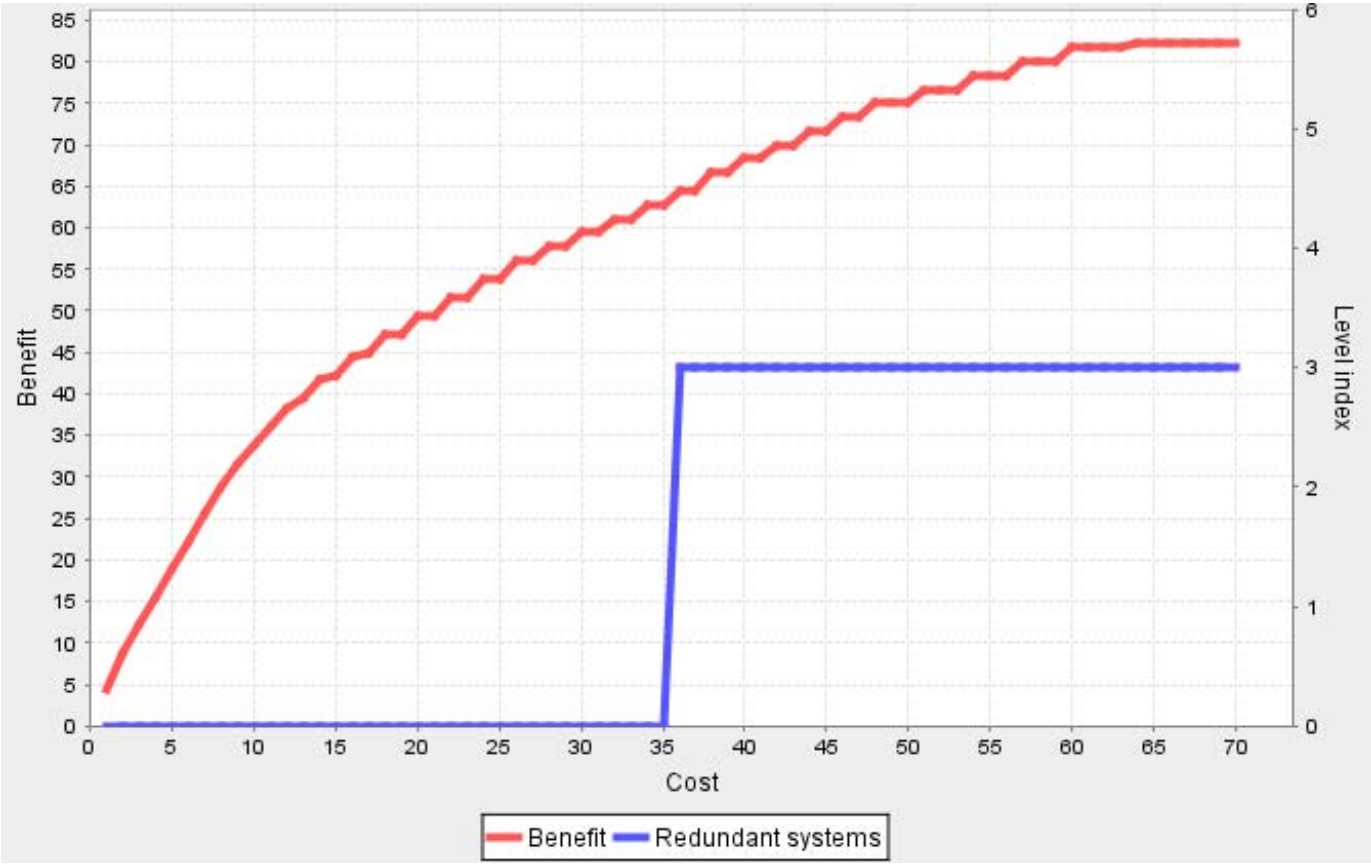

RunSchemeEditor.bat
C:\CoCoViLa_Inteligentne programmeerimi
vila-0.6.4-dev>rem @echo off
C:\CoCoViLa_Inteligentne programmeerimi
exampledp-multi - CoCoViLa - Scheme Edito
File Edit Package Scheme Options Help
optimization
DynamicOptimizer_0 - optimization
Object name Optimizer_0 (String) Input Goal Watch
minbudget 1 (int)
maxbudget 70 (int)
maxcost (int)
maxbenefit (double)
Static
OK Clear all
User training
0 0
4 30
8 60
12 65
Antivirus
0 0
2 60
4 80
7 95
Encryption
0 0
2 60
4 80
7 95
1 70
0
30
50
65
S
y
sion detection
0
25
45
60
MeasureGroup_6 - optimization
Object name MeasureGroup_6 (String) Input Goal Watch
description Encryption (String)
costs 0 (int[])
benefits 0 (int[])
optimal (int)
s1 (double)
s2 (double)
s3 (double)
weight 1.0 (double)
Static
OK Clear all
06h 07h 08h 09h 10h 11h


exampledp-multi - CoCoViLa - Scheme Editor
File Edit Package Scheme Options Help
optimization
100%
User training
0 0
4 30
8 60
12 65
Antivirus
0 0
2 60
4 80
7 95
Encryption
0 0
2 60
4 80
7 95
1 70
Redundant systems
0 0
8 40
10 70
12 95
Backup
Firewall
Access co
0 0
1 40
2 70
4 95
166, 17
21h
22h
Graph
Benefit
Level index
Cost
Benefit
User training
Firewall
Intrusion detection

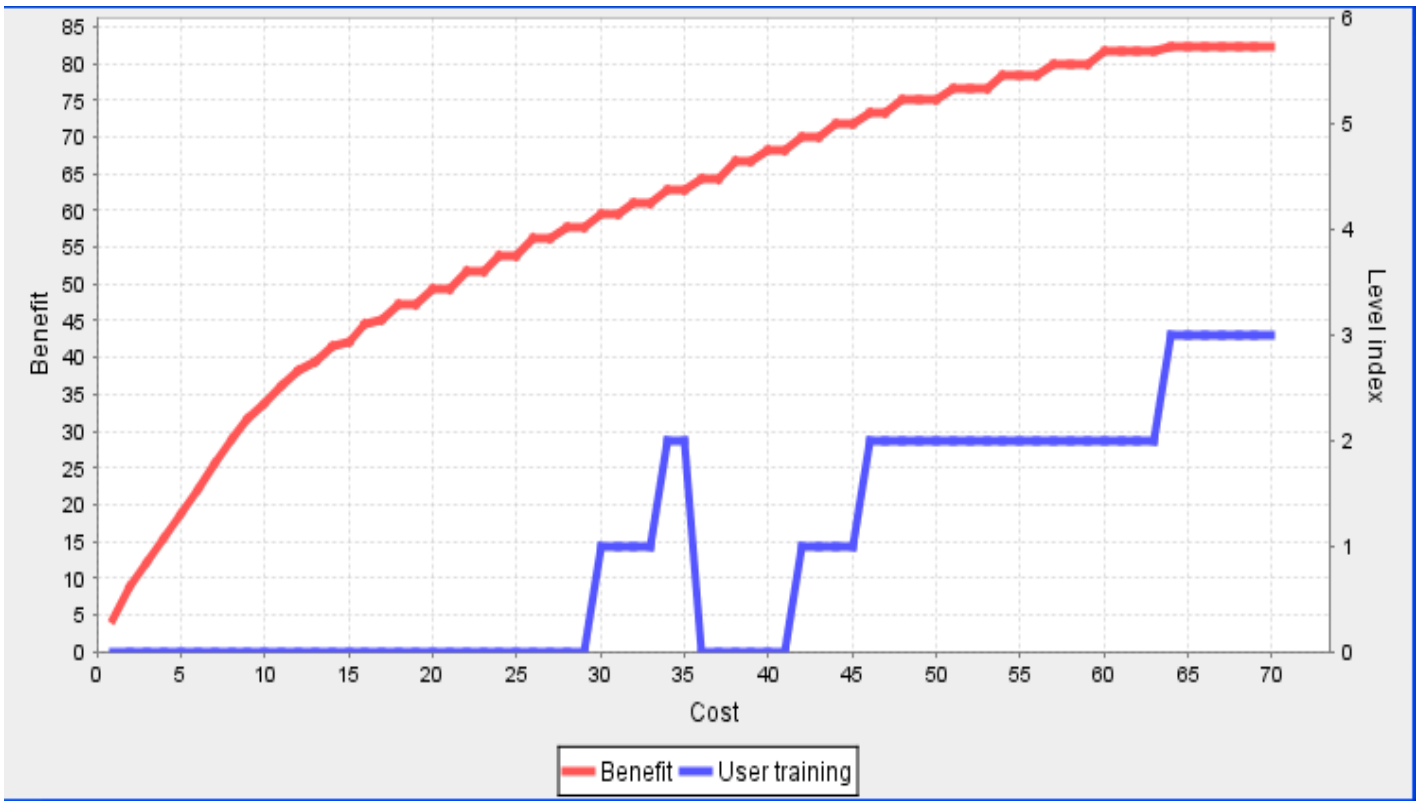
CoCoViLa - optimumi kõver ja Antiviirus



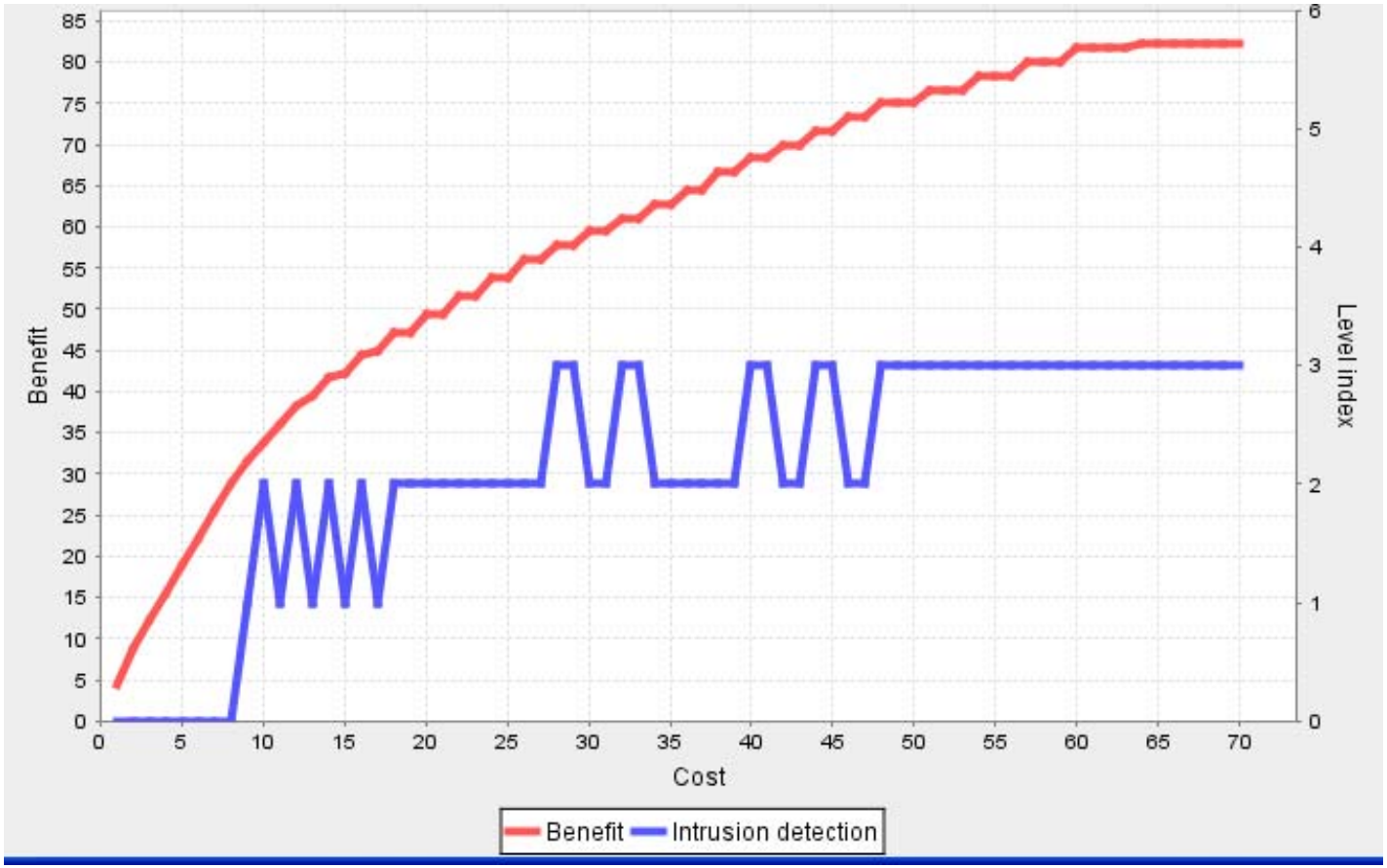
CoCoViLa - optimumi kõver ja Dubleerimine



CoCoViLa - optimumi kõver ja Kasutajate Koolitus

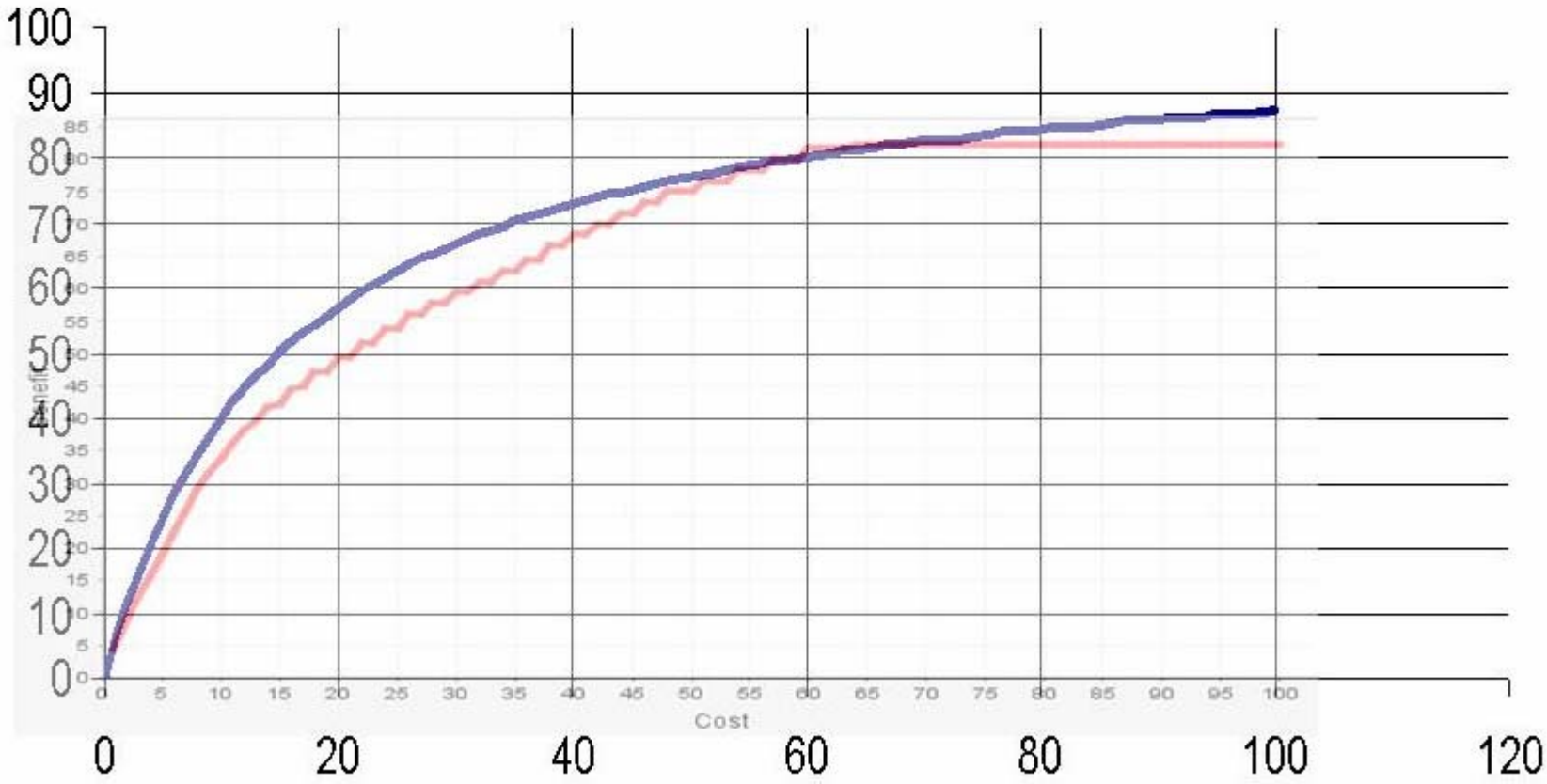


CoCoViLa - optimumi kõver ja IDS

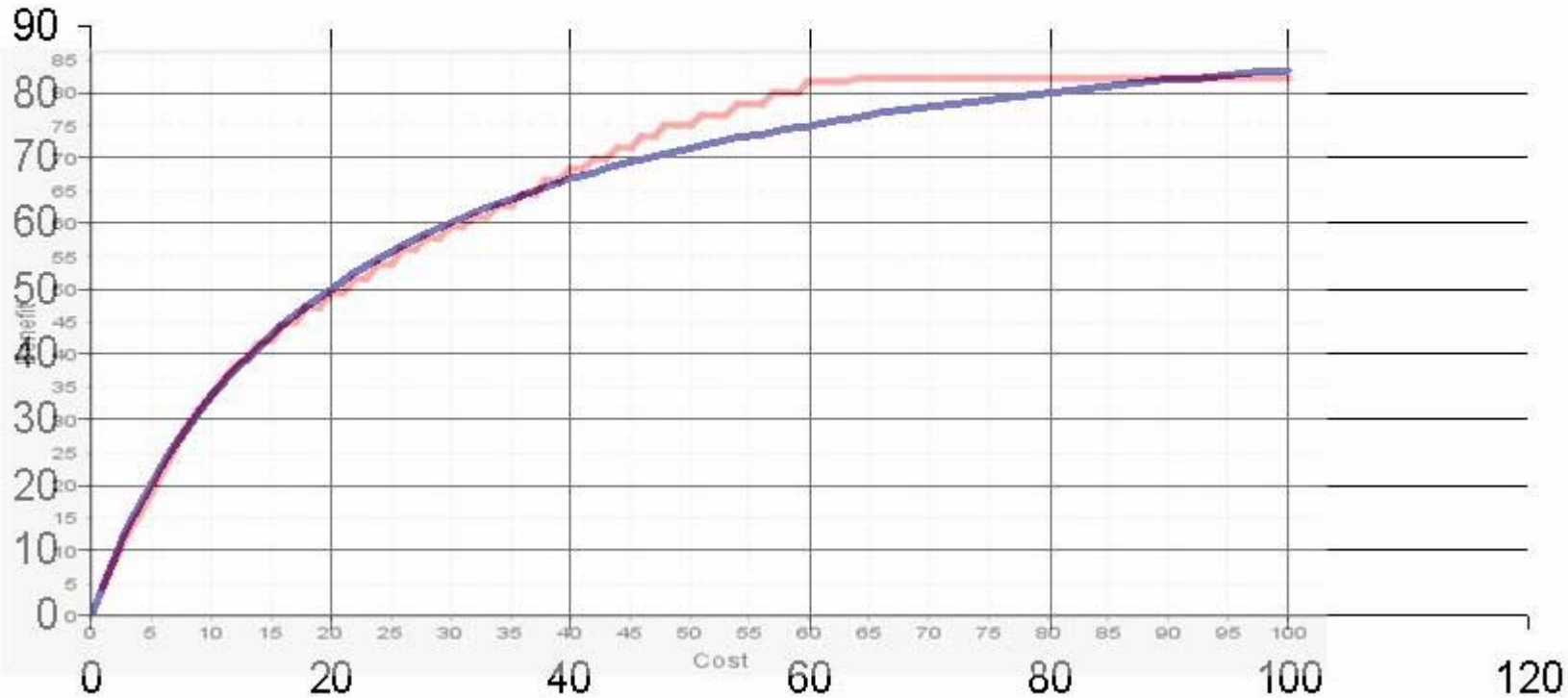


Ühtlasi tekkis võimalus kontrollida, et kas infoturbe valdkonnas on Monod' funktsiooni kasutamine õigustatud – st kas Monod' ja kulutuste optimaalsuse kõverad langevad kokku?

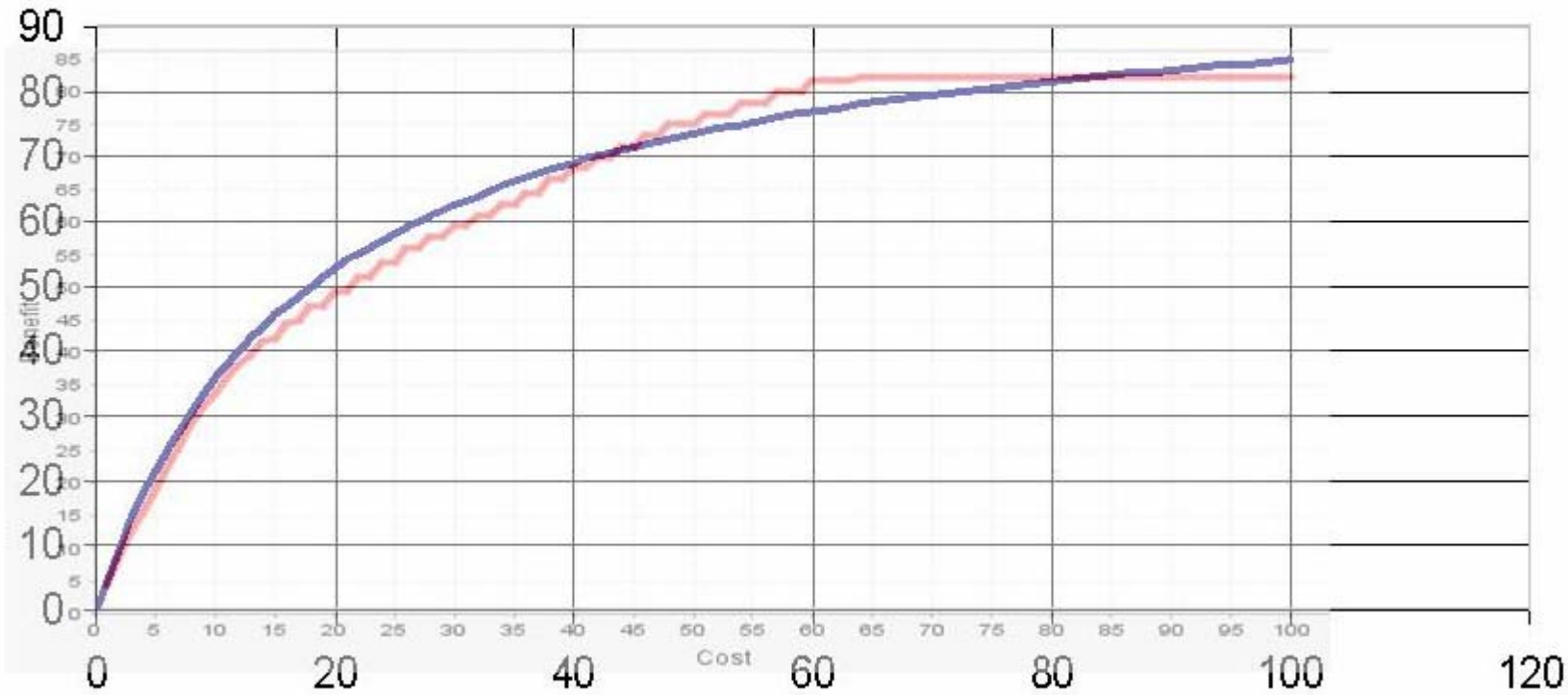
Monod' kasvufunktsioon y=ax/(k+x) [konkreetne kõver on y=100x/(15+x)] ja CoCoViLa andmeturbe optimaalsete kulutuste kõver



Monod' kasvufunktsioon y=ax/(k+x) [konkreetne kõver on y=100x/(20+x)] ja CoCoViLa andmeturbe optimaalsete kulutuste kõver



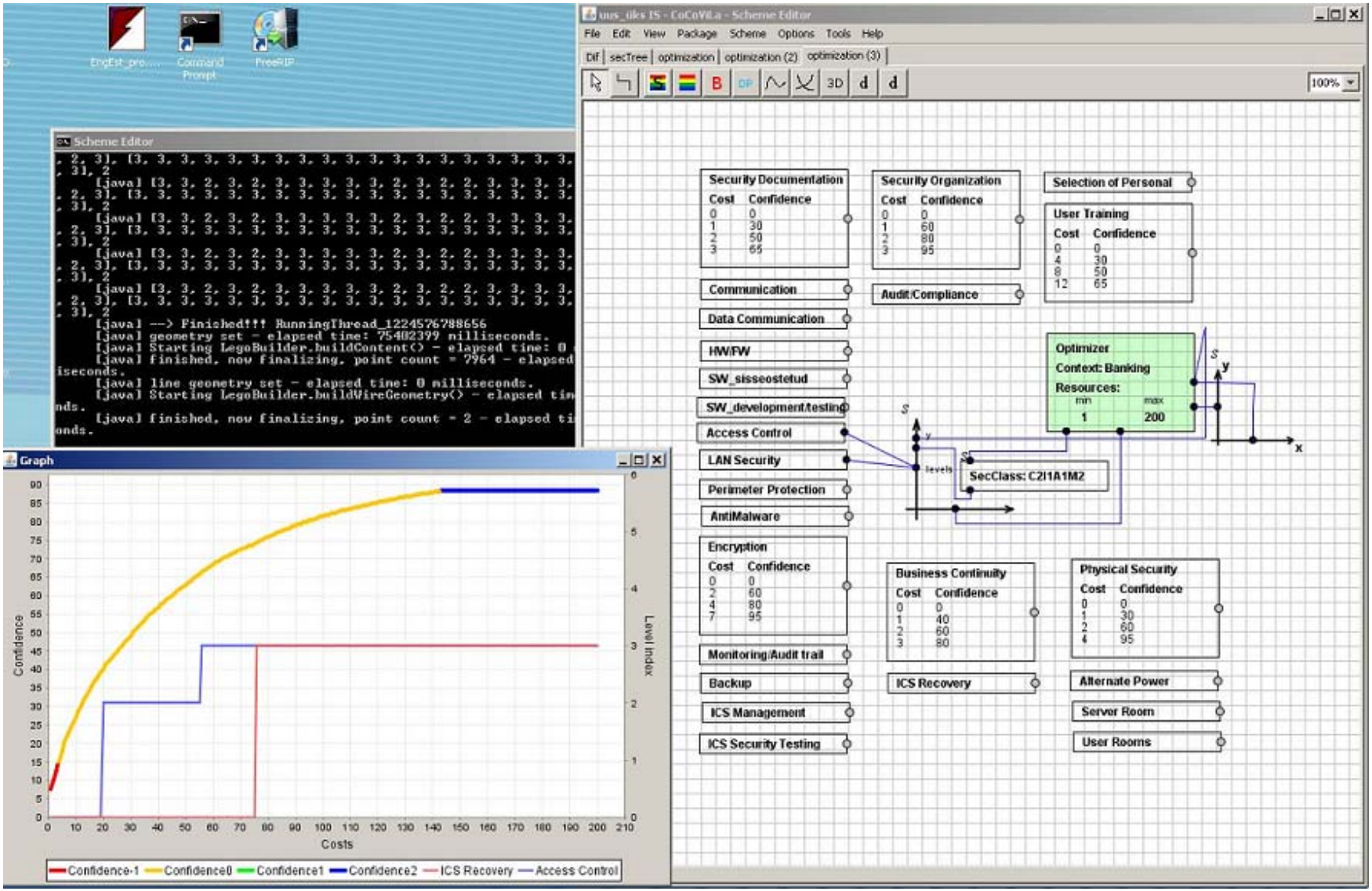
Monod' kasvufunktsioon y=ax/(k+x) [konkreetne kõver on y=100x/(18+x)] ja CoCoViLa andmeturbe optimaalsete kulutuste kõver



Max hälve < 5%

Nagu näha, k=18-korral on kõverate erinevus alla 5%. Loeksin seda julgustavaks märgiks – liigume ilmselt õiges suunas.

Graded Security Expert System'i viimastest arengutest


Scheme Editor
[java] Finished!!! RunningThread_1224576788656
[java] geometry set - elapsed time: 75402399 milliseconds.
[java] Starting LegoBuilder.buildContent() - elapsed time: 0
[java] finished, now finalizing, point count = 7964 - elapsed
iseconds.
[java] line geometry set - elapsed time: 0 milliseconds.
[java] Starting LegoBuilder.buildWireGeometry() - elapsed tim
nds.
[java] finished, now finalizing, point count = 2 - elapsed ti
onds.
Graph
Confidence
Level Index
Costs
Confidence-1
Confidence0
Confidence1
Confidence2
ICS Recovery
Access Control
File Edit View Package Scheme Options Tools Help
Dif secTree optimization optimization (2) optimization (3)
100%
Security Documentation
Cost Confidence
0 0
1 30
2 50
3 65
Security Organization
Cost Confidence
0 0
1 60
2 80
3 95
Selection of Personal
User Training
Cost Confidence
0 0
4 30
8 50
12 65
Communication
Audit/Compliance
Data Communication
HW/FW
SW_sisseostetud
SW_development/testing
Access Control
LAN Security
Perimeter Protection
AntiMalware
Optimizer
Context: Banking
Resources:
min max
1 200
levels
SecClass: C2I1A1M2
Encryption
Cost Confidence
0 0
2 60
4 80
7 95
Business Continuity
Cost Confidence
0 0
1 40
2 60
3 80
Physical Security
Cost Confidence
0 0
1 30
2 60
4 95
Monitoring/Audit trail
Backup
ICS Recovery
Alternate Power
ICS Management
Server Room
ICS Security Testing
User Rooms

Optimeerimismeetodist:

- **jõumeetodil** optimumi otsides peaksime läbi proovima **qk^n** punkti/arvutust,
- **Pareto dünaamilise programmeerimise meetodil q^2kn,**

  kus q - vahemike/punktide arv,

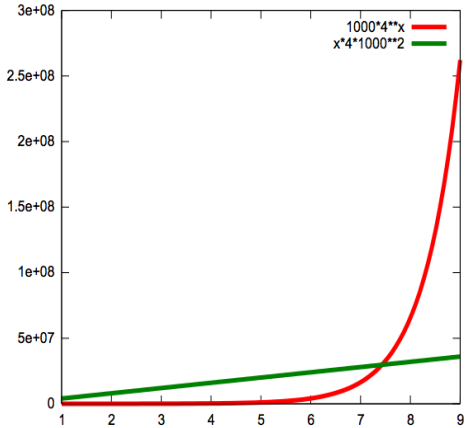
  k - ressursi/turvavaldkonna erinevate võimalike väärtuste arv,

  n - käsitlevate ressursside/turbevaldkondade arv

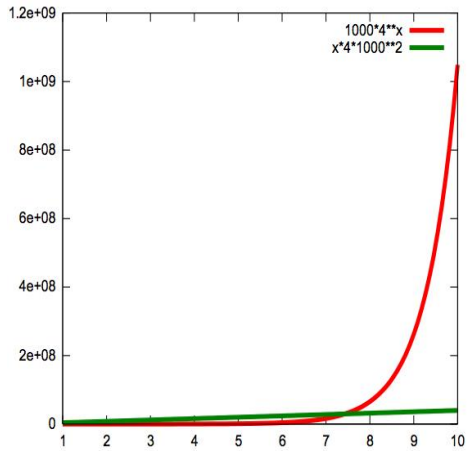
  st BruteForce'iga arvutusmaht kasvab n-i suhtes eksponentsiaalselt ja Pareto'ga lineaarselt

  Näiteks kui q=100, k=4 ja n=25, siis jõuga ~10^{17} ja Pareto'ga ~10^6 arvutust,

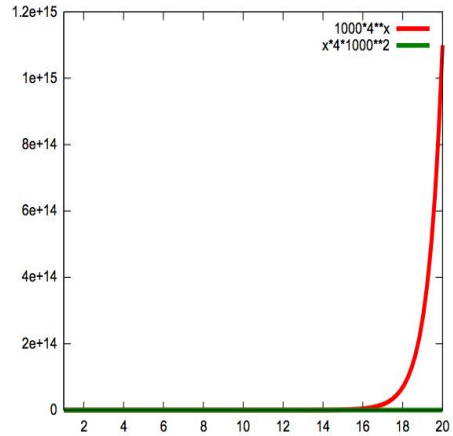
  st Pareto's arvutus võtab aega mõned sekundid (5÷10) ja BruteForce'is ~200÷300 aastat.
- **kui Pareto-meetodiga arvutades jagame uuritava vahemiku näiteks 100-ks ja 1000-ks (st q=100 ja q=1000), siis nende kahe juhu arvutusaeg erineb 100x – sest sõltuvus ju q^2**



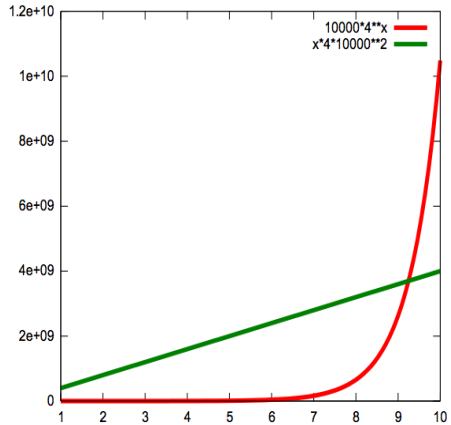
Joonis ... 1000x9



Joonis ... 1000x10



Joonis ... 1000x20



Joonis ... 10000x10

Kaalutud keskmisest.

Infoturbe tegevusvaldkondade vaheliste sõltuvuste kirjeldamisega tegeletakse küllalt laialdaselt – üritatakse luua nn Dependency Model/Dependency Graph'e. Väljakujunenud laialdasemalt aktsepteeritud lahendusi veel ei ole, mis on ka põhjuseks, et oma optimeerimismudelis esialgu kasutame kaalutud keskmist. Seda võib käsitleda kui Dependency esimest oluliselt lihtsustatud versiooni.

Kaalutud keskmises määratletakse infoturbe tegevusvaldkondade kaalud info turvaeesmärkide kaalude kaudu.
Näiteks: kui info salastatuse kaal $K_C=2$ ja $K_I=3$, $K_A=1$, siis kui mingi infoturbe tegevusvaldkond tegeleb/tagab nii info Salastatust, terviklust kui ka käideldavust, siis tema kaal

$$K_{CIA} = \text{normaliseeritud } K_C K_I K_A$$

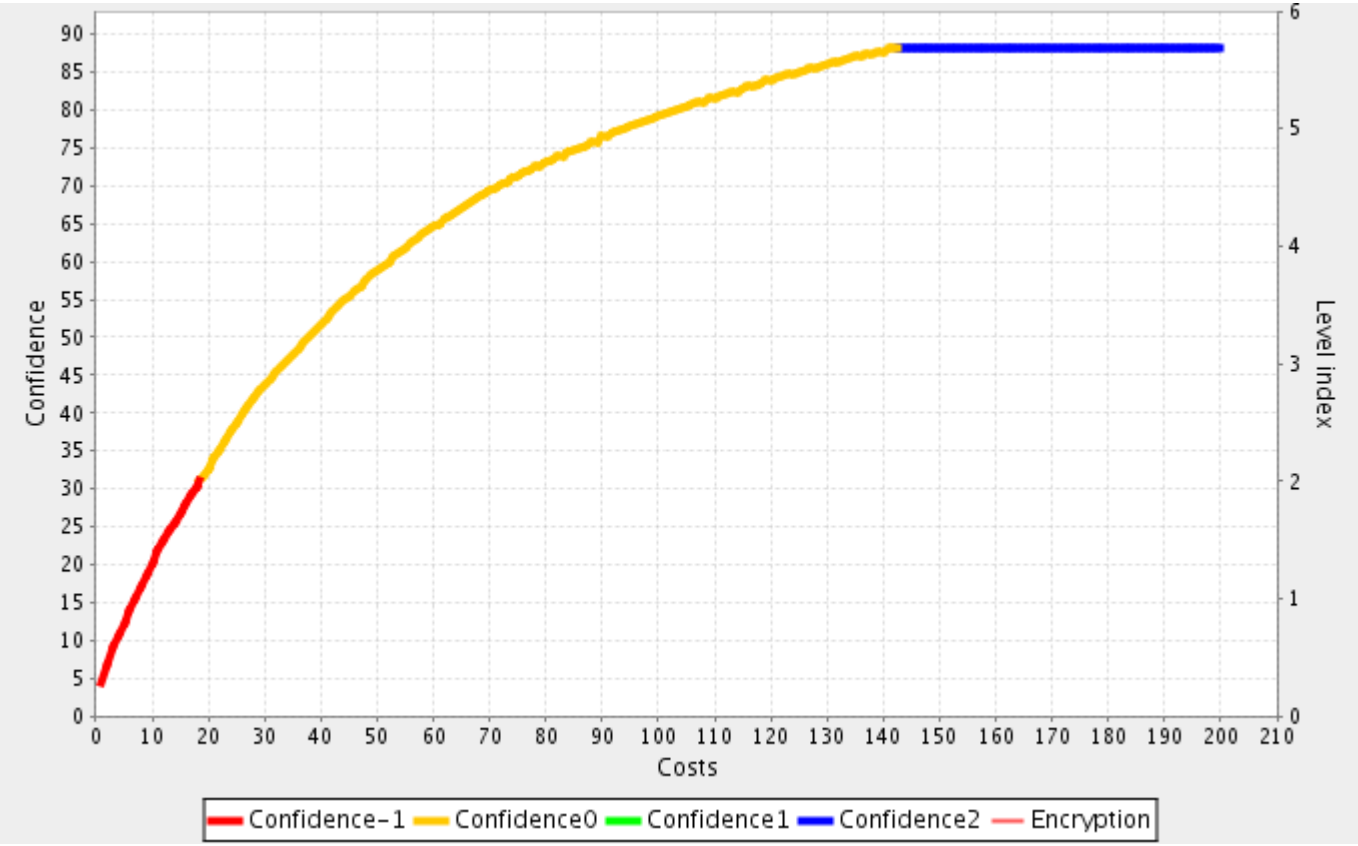
Security activities subareas	Kaal					
	K_C=1,5 K_I=2 K_A=1	$K_C K_I K_A$	K_{CIA}	Ühiskasutatavus K_U Ühine K_U=0,25 Ühine+spetsiifiline K_U=0,5 IS spetsiifiline K_U=1	Lõplik $K_C K_I K_A K_U$	K_{CIAU}
Turvaorganisatsioon, -strateegia, -poliitika	1	1	0,724638	0,25	0,25	0,359712
Turbe audit/vastavus/akrediteerimine	CI	3	2,173913	0,5	1,5	2,158273
IT Personalihaldus	1	1	0,724638	0,5	0,5	0,719424
Personali (turva)koolitus User Training	1	1	0,724638	0,25	0,25	0,359712
Füüsiline turve	1	1	0,724638	0,25	0,25	0,359712
Alternatiivne toide	1	1	0,724638	0,25	0,25	0,359712
Serveriruumid	1	1	0,724638	0,25	0,25	0,359712
IS lõppkasutajate tööruumid	1	1	0,724638	0,25	0,25	0,359712
Side (telefon, mobiil jms)	1	1	0,724638	0,25	0,25	0,359712
Andmeside	C	1,5	1,086957	0,5	0,75	1,079137
. . . .						
Äri(põhitegevus)protsesside talitluspidevus ja taaste	1	1	0,724638	1	1	1,438849
Infosüsteemide taaste Redundant Systems	CA	1,5	1,086957	0,5	0,75	1,079137
Normaliseerimine		34,5	25		17,375	25

Optimaalsuse kõvera väljajoonistamisest.

Sisuliselt on optimaalsuse kõveral mitu sisuliselt erinevat lõiku:

- **lõik, kus IS turvatase ja praktiliselt kõigi turbe tegevusvaldkondade turvatasemed on alla nõutu;**
- **lõik, kus IS turvatase ja kõigi turbe tegevusvaldkondade turvatasemed on võrdsed nõutavaga;**
- **lõik, kus IS turvatase ja praktiliselt kõigi turbe tegevusvaldkondade turvatasemed on üle nõutu.**

Eesmärgiks ainult maksimaalne Confidence:

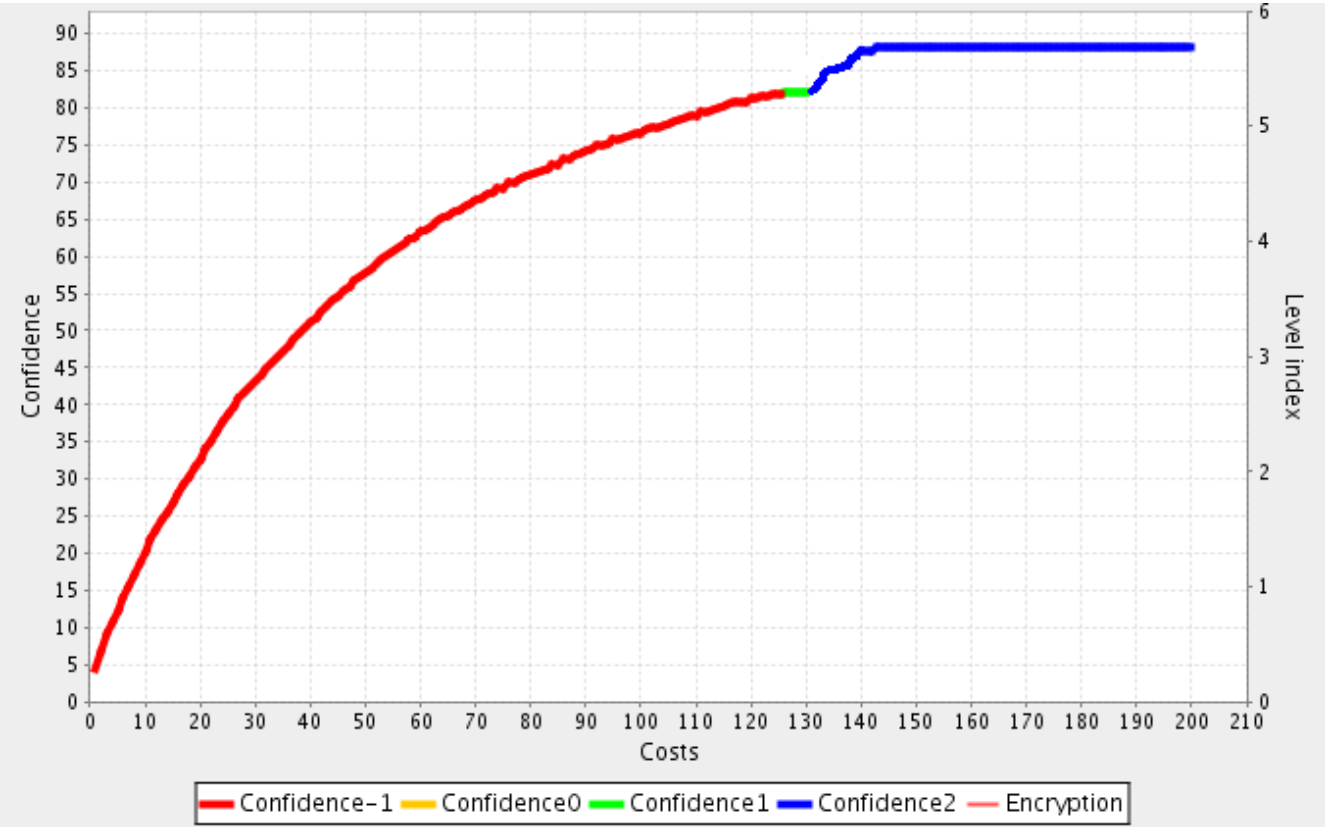


Punane joon: turvatase kõigis turbe valdkondades ≤ nõutavast ja vähemalt ühes < nõutavast
Roheline joon: kõigis turbe valdkondades turvatase =nõutavaga
Kollane joon: mõned turvatasemed alla ja mõned üle nõutava
Sinine joon: turvatase kõigis turbe valdkondades ≥ nõutavast ja vähemalt ühes > nõutavast

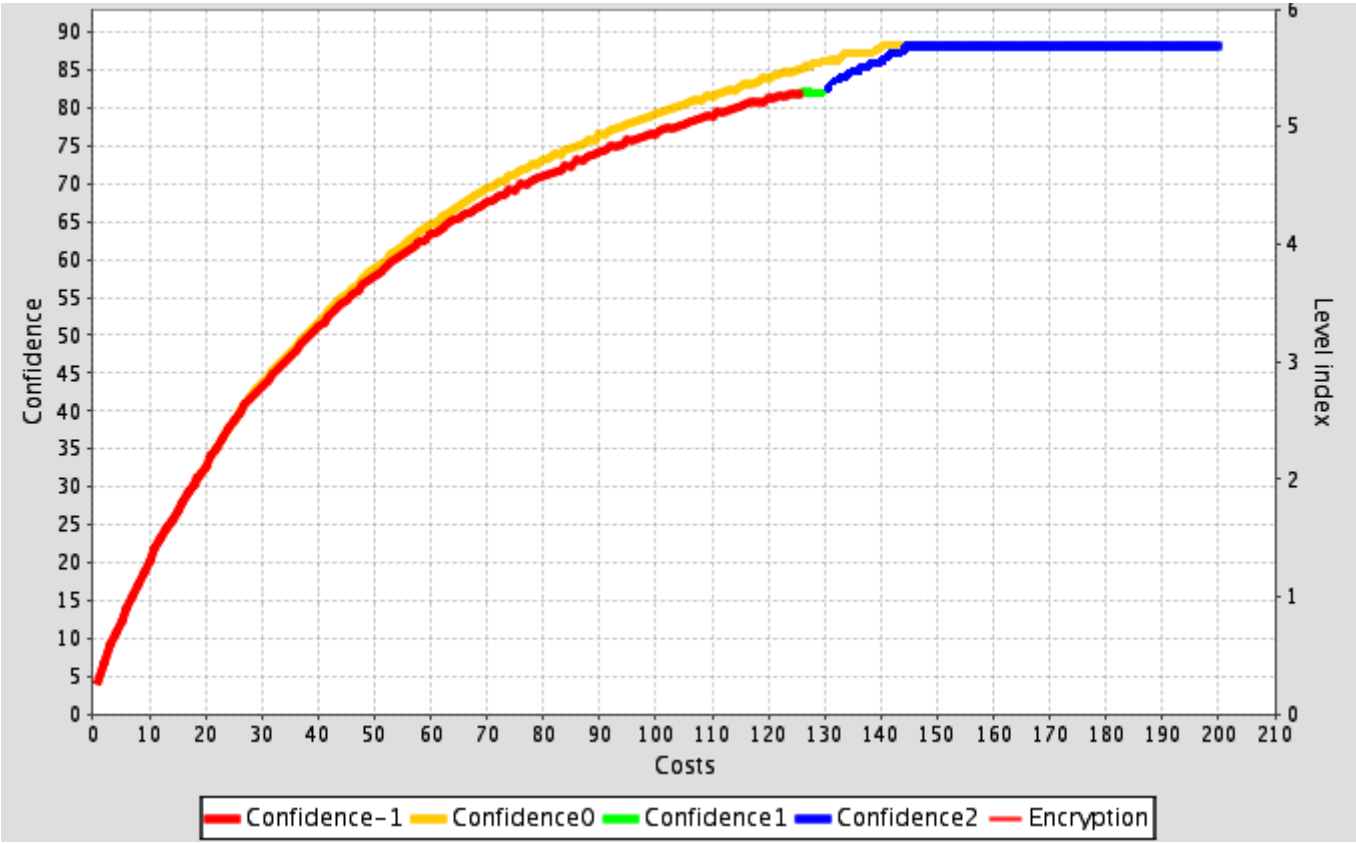
Tegelik lootus oli, et tulemuseks saame hoopis midagi sellist:

Eesmärgiks maksimaalne Confidence, kuid sisse toodud kaks piirangut:

- **kuni nõutava turvataseme saavutamiseni (roheline punkt/lõik) ei tohi ühesgi turbe valdkonnas nõutavat turvataset ületada;**
- **Kui nõutav turvatase on saavutatud, siis edasi ei tohi ühegi turbe valdkonna tase langeda allapoole nõutavat**



Võrdleme kahte eelnevat kõverat:



Eelnevat kokku võttes - valmis hakkab saama infoturbe esimese aasta kulutuste mudel.
Vajalik veel põhiliselt ekspertteadmiste kogumine.

Tööd jätkub pikemaks:

- **IS turbe kulud järgmistel aastatel;**
- **infoturbe kulud ja nende mõttekus/optimaalsus asutuse/ettevõtte kogu integreeritud infosüsteemi (IIS) tasemel;**

- **infoturbe valdkondade *Dependency model/graph;***
- **ründe graaf/-puu;**
- **IS turbe kahjude kõver/funktsioon.**

Kokkuvõtteks:

Infoturve pole veel teadus, kuid ta pole enam ka mustkunst, kus loogilise mõtlemisega poleks eriti midagi peale hakata.

Visalt infot kogudes/otsides ja probleemidele süsteemselt lähenedes on võimalik tõele küllaltki lähedale jõuda.

Ehk on eelnevalt käsitletu abiks tulevastes võitlustes ressursside pärast ?

???

Tänan !